

**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF TEXAS  
HOUSTON DIVISION**

IN THE MATTER OF APPLICATION	§	
FOR CELL TOWER RECORDS	§	MAGISTRATE NO. H-15-136M
UNDER 18 U.S.C. § 2703(D)	§	

**OPINION**

On February 10, 2015 the Government filed this application under section 2703(d) of the Stored Communications Act seeking somewhat unusual authority – an order compelling seven different cell phone service providers to release historical cell tower data for specific towers providing service to a crime scene within Houston city limits at the hour of the crime. What is unusual is that, unlike most requests for account records under the SCA, the targeted account is not specified; neither the phone number nor the identity of the phone’s subscriber or customer are currently known to law enforcement. By obtaining the records of all wireless devices using a nearby tower at the time of the crime, the Government hopes to identify the particular device used by the suspect and any confederates, and ultimately to enable their capture and arrest.

This court granted the application, but modified the requested time window from one hour to ten minutes. Because there is contrary authority in this district as to the propriety of such orders (sometimes called “cell tower dumps”) under the SCA, the court issues this opinion to explain its rationale.

### **Background**

Earlier this year in Houston, a private security video recorded an unknown individual approaching a commercial business location on foot, holding a wireless device to his ear. A minute later he lowered the device from his ear, pausing to look at it before putting it in his pocket. He then entered the business, committed a crime, and fled the scene minutes later. The relevant portion of the video-recorded sequence is about 6 minutes long.

The Government seeks historical cell-tower log information from the towers in the vicinity of the business while the crime was in progress. These records may include the telephone call numbers and unique identifiers for any wireless device communicating via that tower; the source and destination telephone numbers for those communications; the date, time and duration of each communication; the tower sector handling the radio signal; and the type of communication (such as phone call or text message). The Government also seeks subscriber account information for the telephone numbers revealed by the cell tower log. The request does not seek precise location data, nor does it seek to track the movements of a particular cell phone over time.

### **Analysis**

Few published opinions treat the subject of cell tower dumps. Three such opinions were issued by my colleague in Corpus Christi, Magistrate Judge Brian Owsley. *In re Application for an Order Pursuant to 18 U.S.C. § 2703(D)*, 964 F. Supp. 2d 674 (S.D. Tex. 2013); *In the Matter of the Search of Cellular Telephone Towers*, 945 F. Supp. 2d 769 (S.D.

Tex. 2013); *In re Application for an Order Pursuant to 18 U.S.C. § 2703(D)*, 930 F. Supp. 2d 698 (S.D. Tex. 2012). The gist of these decisions is that (1) as a constitutional matter, the records sought are protected by the Fourth Amendment, and therefore a warrant based on probable cause is required to access them; and (2) as a statutory matter, the Stored Communications Act does not authorize this type of request.

More recently, a magistrate judge in New York reached the opposite conclusion on both the constitutional and statutory issues. *In the Matter of Application For an Order to Disclose Cell Tower Log Information*, No. M-50, 2014 WL 4388397 (S.D.N.Y. May 30, 2014) (Magistrate Judge James Francis IV). As explained below, I am constrained by binding Fifth Circuit authority to agree with Judge Francis on the Fourth Amendment question. As for the matter of statutory interpretation, I concur with Judge Francis's analysis and conclude that the SCA authorizes the compelled disclosure of cell tower log data.

# **1. Cell Tower Logs and the Fourth Amendment**

The tower dump opinions by Judge Owsley were issued before the Fifth Circuit decided *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013). In a 2-1 opinion, that Fifth Circuit panel held that orders for historical cell site records under the SCA did not “categorically” violate the Fourth Amendment. The panel majority reasoned that cell site records were ordinary business records of the provider in which the customer had no reasonable expectation of privacy<sup>1</sup> – notwithstanding a 1999

---

<sup>1</sup> *Historical Cell Site Data*, 724 F.3d at 611-15.

federal statute declaring that call location records belonged to the *customer* as “customer proprietary network information,” and could not be used, disclosed or accessed “without the express prior authorization of the customer.”<sup>2</sup>

The panel majority emphasized that its decision was a narrow one, and among other things expressly declined to address “orders requesting data from all phones that use a tower during a particular interval.” 724 F.3d at 615. Even so, the Fifth Circuit’s reasoning leaves no doubt that the cell tower logs requested here would likewise be categorized as ordinary business records entitled to no constitutional protection. Unlike call location records, no federal statute confers upon the customer any proprietary rights in her cell phone number or account information. Having disregarded the customer’s statutorily-conferred proprietary rights in location records held by the provider, there is no reason to believe the Fifth Circuit would rule differently for records such as these, which are not the property of the customer. If the customer has no reasonable expectation of privacy in call location records, it follows *a fortiori* that he has no reasonable expectation of privacy in his phone number or account records.

---

<sup>2</sup> Wireless Communication and Public Safety Act (WCPSA), 47 U.S.C. § 222(f)(1). The court’s opinion dealt with this WCPSA argument in a terse footnote, observing that “the SCA is a statute as well” and provides no special protection for (indeed, does not even mention) call location data. 724 F.3d at 609 n.10. The obvious rejoinder – that the specific language of the WCPSA should prevail over the general language of the SCA – was not considered. *See, e.g., Navarro-Miranda v. Ashcroft*, 330 F.3d 672, 676 (5th Cir. 2003) (“As a fundamental rule of statutory interpretation, specific provisions trump general provisions.”).

The net effect is that the Fourth Amendment ground for Judge Owsley's rulings on cell tower dumps has been cut away, at least for the time being,<sup>3</sup> in this circuit. We now turn to the statutory ground for these rulings.

## **2. Cell Tower Logs and the Stored Communications Act**

The Stored Communications Act does not use the term "cell tower dump." However, the tower logs sought here will yield types of records expressly listed in that statute, including "telephone or instrument number or other subscriber number or identity" and "local and long distance telephone connection records, or records of session times and durations." 18 U.S.C. § 2703(c)(2).<sup>4</sup> That said, it is true that this application differs from the typical §2703(d) application in a significant respect – the manner in which the sought-after records are targeted or "selected."

---

<sup>3</sup> See *United States v. Guerrero*, 768 F.3d 351, 357-61 (5th Cir. 2014) (acknowledging that the *Historical Cell Site* holding was arguably called into doubt by the Supreme Court's cell phone search opinion in *Riley v. California*, 134 S. Ct. 2473 (2014)).

<sup>4</sup> The full text of the relevant subsection reads:  
A provider of electronic communication service . . . shall disclose to a governmental entity the —  
(A) name;  
(B) address;  
(C) local and long distance telephone connection records, or records of session times and durations;  
(D) length of service (including start date) and types of service utilized;  
(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and  
(F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

In the usual § 2703(d) application, the Government requests account records associated with a particular phone number, or the name of a particular subscriber or customer, or both. This typically results in the production of a set of records pertaining to a single account. Here, by contrast, the “selector” is the cell tower in contact with all mobile devices at a given time, which might retrieve several thousand phone numbers in a metropolitan area like Houston. The question arises whether or not the SCA contemplates a single order compelling access to records from multiple accounts.

In a letter brief to Judge Francis, the ACLU argued in the negative, pointing out that the SCA is consistently phrased in the singular, and repeatedly refers to records pertaining to “a subscriber to or customer of such service.”<sup>5</sup> However, this argument is effectively refuted by the Dictionary Act, which instructs courts that “[i]n determining the meaning of any Act of Congress, unless the context indicates otherwise, words importing the singular include and apply to several persons, parties or things; [and] words importing the plural include the singular. . . .” 1 U.S.C. §1. Thus the default rule of interpretation is to include both singular and plural, absent a contrary indication in the statute.<sup>6</sup>

---

<sup>5</sup> See ACLU Letter Brief of May 20, 2014, available at <https://www.aclu.org/national-security/aclu-tower-dump-brief> (last visited March 9, 2015).

<sup>6</sup> The ACLU cited an early case for the somewhat different proposition that the rule “is not one to be applied except where it is necessary to carry out the evident intent of the statute.” *First Nat’l Bank in St. Louis v. Missouri*, 263 U.S. 640, 657 (1924). However, that case construed an earlier version of the Dictionary Act, which implied court discretion rather than a default rule: “[W]ords importing the singular number *may extend and be applied to* several persons or things.” *Id.* (citing Rev. Stat. § 1). The Act was amended to its current form in 1948. 62 Stat. 859 (June 25, 1948).

Nothing in the context of the SCA suggests an intent to rule out the plural. One passage in the SCA does mention “unusually voluminous” requests:

A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are *unusually voluminous* in nature or compliance with such order otherwise would cause an undue burden on such provider.

18 U.S.C. § 2703(d) (emphasis added). But this passage does not limit a records request to a single account or phone number. To the contrary, the reference to “unusually voluminous” requests implies that a merely “voluminous” request, perhaps encompassing multiple accounts, is within the contemplation of the law.

Moreover, the court’s power to quash a voluminous request is triggered by “a motion made promptly by the service provider,” suggesting that the initial judgment about what is too voluminous is the provider’s call, not the court’s. To be sure, the court has inherent power to limit the scope of the tower dump based on Fourth Amendment privacy concerns, but again, the Fifth Circuit has found no reasonable expectation of privacy in cell site records.<sup>7</sup> A court could also limit the temporal scope of the tower dump based on the Government’s threshold showing of the “specific and articulable facts” required by § 2703(d). For that very reason, I have reduced the relevant time window here from one hour to ten minutes. These considerations do not defeat or undermine the Government’s position that at least some volume of multiple account records is accessible under a single § 2703(d) order.

---

<sup>7</sup> *Historical Cell Site Data*, 724 F.3d at 611-15.

Accordingly, I concur with Judge Francis that the SCA authorizes law enforcement access to cell tower logs and associated account information.

### **3. Cell Tower Logs vs. Cell Site Simulators**

A further word is necessary to avoid possible misunderstanding. This holding has no application to a related though very different investigative technique using a device known as a cell site simulator, sometimes referred to as a “StingRay.” Like a cell tower dump, the StingRay device may be used to discover telephone and other identification numbers of wireless devices in a given location. However, there are several critical differences: (1) the device is deployed by law enforcement, not the provider; (2) the information obtained is transmitted in real time directly to law enforcement, not retrospectively via the provider’s records; and (3) the device allows continuous real time tracking of the wireless devices in contact with it.<sup>8</sup>

There is little reported case law considering the governing statutory authority for law enforcement’s use of a StingRay device. In the only reported case from this district, Judge Owsley denied the government’s application to authorize such a device under the Pen/Trap Statute. *In re Application for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747 (S.D. Tex. 2012). Law enforcement had intended to use the device to identify the telephone number of a cell phone used by a

---

<sup>8</sup> See Stephanie Pell & Christopher Soghoian, *A Lot More Than a Pen Register and Less Than a Wiretap: What the StingRay Teaches About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J. L. & Tech. 134, 144-48 (2014).



suspected drug dealer. But as Judge Owsley persuasively observed, the Pen/Trap Statute requires that a pen/trap order must specify in advance “the number or other identifier” of the targeted phone, in contrast to other information which need be specified only “if known.” *Id.* at 751 (citing 18 U.S.C. § 3123(b)(1)). In other words, Congress did not contemplate that a pen/trap order could be used to discover the phone number of the *target* phone.

Another case suggests that a mobile tracking device warrant under Rule 41 of the Federal Rules of Criminal Procedure is the proper procedure for a cell site simulator, at least when the device is used to track the location of a target device. *See United States v. Rigmaiden*, 844 F. Supp. 2d 982, 995 (D. Ariz. 2012). The defendant, a fugitive charged with identity theft, was located by a cell site simulator that “mimicked a Verizon Wireless cell tower and sent signals to, and received signals from, the aircard” connected to his laptop computer. The government had obtained a Rule 41 mobile tracking device warrant for the cell site simulator,<sup>9</sup> and conceded for purposes of defendant’s motion to suppress that “the aircard tracking operation was a Fourth Amendment search and seizure.” *Id.*

Neither case considered whether the Stored Communications Act could authorize the use of a cell site simulator, and for good reason. The SCA is a record production regime, authorizing one-time access to account records in the hands of the provider, as opposed to the continuous real-time monitoring that a StingRay entails. *See, generally, In re Order*


---

<sup>9</sup> As used in *Rigmaiden*, the cell site simulator easily satisfied the broad definition of “tracking device.” 18 U.S.C. 3117(b) (“[T]he term ‘tracking device’ means an electronic or mechanical device which permits the tracking of the movement of a person or object.”).

*Authorizing Prospective and Continuous Release of Cell Site Location Records*, 31 F. Supp. 3d 889, 894-96 (S.D. Tex. 2014) (“Congress never intended the Stored Communications Act to govern ongoing surveillance.”). Thus, even though the StingRay and the tower dump may both ultimately yield the same information – the number or identifier of the cell phone used by a criminal suspect – the manner of acquiring that information is very different, and entails a very different legal analysis.

For all these reasons, the fact that a cell tower dump may be authorized by the SCA does not imply that a cell site simulator is likewise authorized under the SCA.

Signed at Houston, Texas on March 9, 2015.

  
Stephen Wm Smith  
United States Magistrate Judge